АНАЛИЗ БЕЗОПАСНОСТИ СИСТЕМ ELASTIC STACK, WAZUH И IDS В СЕТЯХ.

Rustamov Alisher Bahodirovich
Associate Professor, University of Information Technologies and Management Gmail: arustamov_88@mail.ru
Hamdamov Asilbek Rauf o‘g‘li
Student at the University of Information Technologies and Management
Toshpulatov Javohir Ravshan o‘g‘li
Student at the University of Information T echnologies and Management

Abstract. *One of the major risks associated with the significant growth and use of information technologies interconnected with the Internet is cybercrime. The alarming increase in cybercrime activity over the years has forced organizations to take defensive measures and always use modern technologies for the same purpose. This article reviews the elastic stack, wazuh and ids systems used to detect and analyze attacks on networks.*

Keywords: *Wazuh, HIDS, Linux , AIX , macOS, Solaris, Windows, Elastic Stack, Suricat, IDS, Kibana, NIDS, NIPS, NSM.*

With the development of information and communication technologies, cybersecurity is becoming a serious problem for individuals, businesses and governments. In a world where everything is on the Internet, ensuring the security of our data is one of the biggest cybersecurity challenges. Therefore, several systems are being used to prevent and detect these situations.

Wazuh is a free and open source host-based intrusion detection system (HIDS). It performs registry analysis, integrity checking, Windows registry monitoring, rootkit detection, time-based alerts, and proactive response. It provides intrusion detection for many operating systems, including Linux, AIX, HP-UX, macOS, Solaris, and Windows. Wazuh has a centralized, cross-platform architecture that allows you to easily monitor and manage multiple systems. A host-based intrusion detection system (HIDS) is a network security system that protects computers from malware, viruses, and other malicious attacks.

Elastic Stack offers a wide range of security analytics capabilities for threat detection, visibility, and incident response. The speed and scale with which Elasticsearch can index and search security-related data allows analysts to do their jobs more efficiently, and the Kibana dashboard provides broad visibility and enables interactive

threat hunting. Machine learning, in turn, can automate the analysis of complex data sets, allowing for the identification of attackers who would otherwise be overlooked.

Popular intrusion detection systems (IDS) such as Wazuh or Suricata use a signature-based approach to threat detection. That is, patterns found in files, logs, and network traffic are compared to a database of patterns known to be associated with malicious activity, and alerts are issued when a match is found. These systems provide a set of rules to analyze and correlate data that typically generates thousands or millions of alerts per day in a production environment. Broadcasting across the entire network can ensure the detection of all possible security events, but it also adds the work of investigating thousands (or millions) of alerts per day. Elastic's machine learning features help reduce risk by automatically identifying outliers. This is a clear use case where signature and anomaly-based technologies complement each other to facilitate threat detection and improve investigation efficiency. Wazuh is an open-source Host-Based Intrusion Detection System (HIDS), typically deployed with the Elastic Stack. It offers log analysis, file integrity monitoring, rootkit and vulnerability detection, configuration assessment, and incident response capabilities. Wazuh's solution architecture is based on lightweight, cross-platform agents that run on monitored systems and send reports to a centralized server where data analysis is performed. It also provides a full Kibana plugin for configuration management, scan monitoring, search, and data visualization. In addition, Suricata is a free, open-source network threat detection engine with real-time network intrusion detection (NIDS), online intrusion prevention (NIPS), network security monitoring (NSM), and offline pcap processing. Suricata inspects network traffic using its own rules and signature language to match known threats, policy violations, and malicious behavior, and offers scripting support for detecting complex threats.

In short. Using signature and anomaly-based attack detection with technologies like Wazuh, Suricata, and Elastic Machine Learning, you can simplify threat detection and improve investigation efficiency.

In turn, integrating host-based IDS (for monitoring host-level systems) with network-based IDS (for inspecting network traffic) can also increase threat detection and security visibility. . Wazuh simplifies this process because it can be used to integrate host and network IDS systems with the Elastic Stack and can provide a mechanism to implement automated responses and block attacks in real time.

REFERENCES:

1. Arora Varul . “ Wazuh: Security Information and Event Management (SIEM) for Small and Medium Enterprises ”.
2. Chernish Anton . “ OSSEC Wazuh, a Security Monitor for Computer Networks ”.
3. Sitorabonu , A. Va Gulmira, P. (2024). KAPARATIV TARMOQLARDA AXBOROT XAVFSIZLIGINI TA'MINLASHDA YANGI TEXNOLOGIYALARNING ROLI. Efiopiya xalqaro multidisipliner tadqiqotlar jurnali, 11(06), 169-171.
4. Qodirov, B. K. (2022). Kredit-modul tizimida ma'lumotlar bazasi fanini o'rganishda muammolarning istiqbollari va ularning echimlari. Xalqaro rasmiy ta'lim jurnali, 2(1), 16-22.
5. Rustamov, A., & Amirov, A. (2022). TARMOQLARDA AUTENTIFIKASIYA PROTOKOLLARIGA QO’LLANILADIGAN NAMUNAVIY HUJUM TURLARI. Прикладные науки в современном мире: проблемы и решения, 1(31), 12-14.
6. Rustamov, A., & Amirov, A. (2022). TARMOQLARDA RANSOMWARENI OLDINI OLISHDA VEB XAVFSIZLIKNING MUHIMLIGI. Прикладные науки в современном мире: проблемы и решения, 1(31), 15-18.
7. Shukrullaevna, N. D., & Bahodirivich, R. A. (2017). MOOC bilan liniyada o'qitish jarayonining sifatini oshirish. Akademiya, 2(6 (21)), 21-24.